Docket No. JP920000150US1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Gupta *et al.*

Group Art Unit: 2143

Filed: 7/27/2000

Examiner: Shin, Kyung H.

Serial No.: 09/626,637

Title: **METHOD AND SYSTEM FOR AUTHENTICATION WHEN CERTIFICATION AUTHORITY PUBLIC AND PRIVATE KEYS EXPIRE**

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REPLY BRIEF OF APPELLANT

This Reply Brief is in reply to the Examiner's Answer mailed on October 10, 2006.

GROUND OF REJECTION 1

Claims 1, 5-6, 11-13, and 17-19 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Lewis et al. (U.S. Patent No. 6,233,565) in view of Weinstein et al. (U.S. Patent No. 6,094,485).

(Note: The Examiner's Answer states that claims 1, 4-6, 11, 13, 17-19 are rejected over Lewis in view of Weinstein, which appears to be a typographical error in light of the claims actually analyzed by the Examiner's Answer over Lewis in view of Weinstein)

Claims 1, 5-6, 13, and 17

Appellants respectfully contend that claims 1, 6, and 13 are not unpatentable over Lewis in view of Weinstein, because Lewis in view of Weinstein does not teach or suggest each and every feature of claims 1, 6, and 13.

A first example of why claims 1, 6, and 13 are not unpatentable over Lewis in view of Weinstein is that Lewis in view of Weinstein does not teach the following first feature: "receiving an original authentication certificate **together** with a server certifying authority chain (SCAC) certificate **by the browser from the server** during a SSL handshake between the browser and the server, said SCAC certificate having been previously obtained by the server from the certifying authority" (emphasis added) (claim 1), and similar language for claims 6 and 13.

The Examiner's Answer cites Lewis, col. 30, lines 39-41, as disclosing the preceding first feature of claims 1, 6, and 13, except for the limitation of receiving the original authentication

certificate and the SCAC certificate together.

As to the limitation of receiving the original authentication certificate and the SCAC certificate together, the Examiner's Answer states: "Lewis does not specifically disclose certificates received together. However, Weinstein discloses: a) receiving an original authentication certificate together with a server certifying authority chain (SCAC) certificate. (see Weinstein col. 3, lines 56-64: multiple (i.e. new, intermediate (i.e. old)) certificates within a transmission (i.e. together)) It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Lewis to enable multiple security client/server certificates transmitted within a network session as taught by Weinstein. One of ordinary skill in the art would be motivated to employ Weinstein in order to optimize encryption within a secure network communications session. (see Weinstein col. 2, lines 10-15: " ... provides a process and apparatus that is used by an exportable version of an SSL client ... negotiate an encrypted communication session using strong encryption with an SSL server ..."".

In response, Appellant will next argue that:

(1) the old certificate and the new certificate are not received **by the browser from the server** as required by claims 1, 6, and 13;

(2) receiving the original authentication certificate and the SCAC certificate together does not make sense for Lewis' invention; and

(3) the argument in the Examiner's Answer for modifying Lewis by the alleged teaching in Weinstein is not persuasive.

Appellants' analysis begins with quoting Lewis, col. 30, lines 36-50:

"**The initial CA's certificate** will be distributed by means of regular US certified

mail. Included with the CA's certificate will be a hash of the next certificate key values. **When a certificate expires, the USPS certification authority will issue a new certificate** and sign it with the old certificates matching private key. The USPS CA will send a new certificate signed with the CA's new private key to the server 4. The server 4 will validate the certificate for authenticity by first checking to ensure that the new CA certificates public key authenticates the included signature. It will then hash the keys included with the new certificate to verify that the hash value match with the old hash included with the old CA's certificate. If both conditions validate, the old CA's certificate is deleted and replaced with a new CA certificate. " (emphasis added).

The preceding quote in Lewis, col. 30, lines 36-50 demonstrates that the old certificate and the new certificate are not received by the browser from the server as required by claims 1, 6, and 13, but are instead received by the server from the Certificate Authority.

The Examiner's Answer (page 18, bottom line - page 19, line 8) argues: "A server is a system that provides a service to a client system. In addition, when a server system receives a service from another system, it becomes a client to that particular system. The server and client roles are interchangeable based on which system is requesting the service and which system is receiving the service."

In response, Appellants assert that the issue of whether a server system can be a server in one situation and a client in another situation is not relevant to Lewis, because in the situation disclosed in Lewis, col. 30, lines 36-50 in which the server 4 receives the old certificate and the new certificate from the Certificate Authority, the server 4 is functioning as a server and not as a client comprising a browser. Moreover, there is no disclosure in Lewis that a browser of the server 4 receives the old certificate and the new certificate from a server.

First, the server 4 in Lewis is serving a plurality of clients 2n as indicated in Lewis, col. 6, lines 49-56 ("FIG. 1 illustrates a system including a customer (also referred to as a "client") 2n, a remote service provider (RSP) 4, and a third party seller of goods and/or services (TPS) 6. The letter "n" is used as a suffix to indicate "one of a plurality of n" such that there may be a plurality of n clients "2" in the system, but the discussion is generally for each client and extends to all clients, although not necessarily identically for each client."). Therefore, the disclosure in Lewis pertains to the server 4 is functioning as a server and not as a client.

Second, Lewis does not disclose anywhere that the server 4 **has a browser**, and surely does not disclose that the server 4 has a browser **that receives the old certificate and the new certificate**, and most certainly does not disclose that the server 4 has a browser that receives the old certificate and the new certificate **from the server**. In Lewis, only the clients 2n have a browser (see Lewis, col. 11, lines 20-22 which teachers that client 2n comprises a browser.)

Therefore, Lewis does not disclose that a browser receives the original authentication certificate and the SCAC certificate together from the server, as required by claims 1, 6, and 13.

The preceding quote in Lewis, col. 30, lines 36-50 also demonstrates that the new certificate replaces the old certificate and thus becomes relevant only after the old certificate expires. Therefore, it makes no sense for the server 4 in Lewis to receive the old and new certificates together, since the server 4 in Lewis already has possession of the old certificate when the server 4 in Lewis receives the new certificate. Thus, it is not obvious to modify Lewis to receive the old and new certificates together.

In addition, the citation in the Examiner's Answer of Weinstein, col. 3, lines 54-60 has no relevance for Lewis. In particular, the multiple certificates in the certificate chain described in Weinstein, col. 3, lines 54-60 are used to verify a server by a client, whereas the old and new certificates described in Lewis, col. 30, lines 36-50 are used to verify a CA certificate by a server.

In addition, the citation in the Examiner's Answer of Weinstein, col. 2, lines 10-15 as allegedly providing motivation to modify Lewis by the alleged teaching of Weinstein is not persuasive. Weinstein, col. 2, lines 10-15 recites: "The invention provides a process and apparatus that is used by an exportable version of an SSL client ... to negotiate an encrypted communication session using **strong encryption** with an SSL server." (emphasis added)

In response, Applicants assert that Weinstein, col. 2, lines 10-15 does not associate use of strong encryption with the feature of Weinstein that the Examiner's Answer relies on to modify Lewis, namely the feature in Weinstein, col. 3, lines 56-64 of transmitting multiple certificates together within a same transmission.

Weinstein, col. 1, lines 35-63, which summarizes how Weinstein's invention enables negotiation of an encrypted session using strong encryption, recites:

> "The invention provides a process, referred to as the SSL step up, which allows an exportable SSL client to negotiate an encrypted session using strong encryption with a server if the server is approved for the step up, i.e. if it is allowed to use strong encryption. It is expected that the same criteria are used to grant this approval as is currently used to grant approval to export special purpose strong encryption software. With the SSL step up process, the SSL client is normally limited to export strength encryption. But, when it is communicating with an approved server, it is able to expand the available set of encryption algorithms to

include stronger algorithms/key lengths.

> The process of the SSL step up involves performing an SSL handshake twice. The process begins when a user desires to establish a session with a server. The client first initiates a network connection to the server. The first handshake between an export client and an approved server results in an SSL session that uses export strength encryption. This establishes a connection using an exportable cipher suite. The client examines the server's certificate obtained as part of the first handshake. If the server is not approved, the SSL session transfers application data that are protected by the export cipher suite. If the server is approved, then the client initiates a second handshake, this time allowing stronger cipher suites. The result of the second handshake is an SSL session that uses strong encryption. The SSL session may then be used to transfer application data that are protected by the strong cipher suite. At this point, the process is complete."

Appellants assert that it is clear from the preceding quote from Weinstein, col. 1, lines 35-63 that the feature in Weinstein, col. 3, lines 56-64 of transmitting multiple certificates together within a transmission is not the basis for the use of strong encryption in Weinstein's invention. Accordingly, Appellants assert that it is not obvious to modify Lewis by the alleged teaching of Weinstein.

A second example of why claims 1, 6, and 13 are not unpatentable over Lewis in view of Weinstein is that Lewis in view of Weinstein does not teach the following second feature: "verifying by the browser the original authentication certificate using the **expired public key** of the certifying authority" (emphasis added) (claim 1), and similar language for claims 6 and 13. The Examiner's Answer argues that Lewis discloses the aforementioned second feature of claims

1, 6, and 13. The Examiner's Answer relies specifically on content disclosed in Lewis, col. 14, lines 36-42 and col. 30, lines 41-43.

In response. Appellants respectfully contend that Lewis col. 14, lines 36-42 does not disclose use of an expired public key of a certifying authority as required by claims 1, 6, and 13 . In fact, Appellants assert that Lewis col. 14, lines 36-42 is irrelevant to the preceding feature of claims 1, 6, and 13.

> In response. Appellants respectfully contend that Lewis, col. 30, lines 39-50 recites: "**When a certificate expires**, the USPS certification authority will issue a new certificate and sign it with the old certificates matching private key. The USPS CA will send a new certificate signed with the CA's new private key to the server 4. The server 4 will validate the certificate for authenticity by first checking to ensure that the new CA certificates public key authenticates the included signature. It will then hash the keys included with the new certificate to verify that the hash value match with the old hash included with the old CA's certificate. If both conditions validate, the old CA's certificate is deleted and replaced with a new CA certificate." (emphasis added).

Appellants assert that the preceding feature of claims 1, 6, and 13 requires verification by the browser using the **expired public key** of the certifying authority, which Lewis does not disclose. There is no mention in Lewis, col. 30, lines 39-50 of use of an expired public key of the certifying authority to validate a certificate. In fact, there is no mention in Lewis, col. 30, lines 39-50 of either an expired public key of the certifying authority or an expired private key of the certifying authority. The only indication in Lewis, col. 30, lines 39-50 of something having expired is mention of an expired certificate. Appellants assert the Examiner's Answer has not provided any citation to Lewis with persuasive accompanying analysis that allegedly discloses

use of an expired public key of the certifying authority to validate any authentication certificate.

Accordingly, Appellants maintain that Lewis does not disclose the preceding feature of claims 1, 6, and 13.

Based on the preceding arguments, Appellants respectfully maintain that claims 1, 6, and 13 are not unpatentable over Lewis in view of Weinstein and are in condition for allowance. Since claim 5 depends from claim 1, Appellants contend that claim 5 is likewise in condition for allowance. Since claim 17 depends from claim 13, Appellants contend that claim 17 is likewise in condition for allowance.

Claims 11 and 18

Since claims 11 and 18 respectively depend from claims 1 and 13, and since Appellants have argued *supra* that claims 1 and 13 are not unpatentable over Lewis in view of Weinstein, Appellants maintain that claims 11 and 18 are likewise not unpatentable over Lewis in view of Weinstein.

In addition with respect to claims 11 and 18, Appellants maintain that Lewis in view of Weinstein does not teach or suggest the feature: "accepting the transaction by the browser after said verifying the original authentication certificate and after said verifying the SCAC certificate" (claim 11), and similar language for claim 18.

The Examiner's Answer argues: "Regarding Claims 11 (New), 18 (New), Lewis discloses the method and system of claims 1, 13 further comprising accepting the transaction by the

browser after said verifying the original authentication certificate and after said verifying the SCAC certificate. (see Lewis col. 27, lines 10-24: verification of a certificate (i.e. server or client) utilizing digital signature techniques with public/private keys)".

In response, Appellants maintain that Lewis, col. 27, lines 10-24 teaches that a user "A" may accept a transaction after verifying an authentication certificate, but does not teach that the user "A" would accept a transaction after verifying **both** the original authentication certificate and the SCAC certificate, as required by claims 11 and 18.

Accordingly, Appellants maintain that claims 11 and 18 are not unpatentable over Lewis in view of Weinstein.

Claims 12 and 19

Since claims 12 and 19 respectively depend from claims 1 and 13, and since Appellants have argued *supra* that claims 1 and 13 are not unpatentable over Lewis in view of Weinstein, Appellants maintain that claims 12 and 19 are likewise not unpatentable over Lewis in view of Weinstein.

In addition with respect to claims 12 and 19, Appellants maintain that Lewis in view of Weinstein does not teach or suggest the feature: "wherein **obtaining** the SCAC certificate comprises using the new private key of the certifying authority" (emphasis added) (claim 12), and similar language for claim 19.

The Examiner's Answer argues: "Lewis disclose the method and system of claims 1, 13, wherein obtaining the SCAC certificate comprises using the new private key of the certifying authority. (see Lewis col. 30, lines 41-43: certificate (i.e. server/client) utilizing private key for

digital signature generation and public key for verification)".

In response, Appellants maintain that Lewis, col. 30, lines 41-43 teaches that the CA signs the new certificate with the CA's private key. In contrast, the "obtaining" in claims 12 and 19 is required to be performed by the server and not by the CA, as may be verified from claims 1 and 13 from which claims 12 and 19 respectively depend. In particular, claim 1 recites: "said SCAC certificate having been previously **obtained by the server** from the certifying authority" (emphasis added). Therefore, Lewis does not disclose "wherein obtaining the SCAC certificate comprises using the new private key of the certifying authority", since the CA who uses new CA's private key is not the server that obtains the SCAC certificate in accordance with claims 12 and 19.

Accordingly, Appellants maintain that claims 12 and 19 are not unpatentable over Lewis in view of Weinstein.

GROUND OF REJECTION 2

Claims 2, 3, 14 and 15 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Lewis-Weinstein and further in view of Perlman *et al.* (US Patent No. 6,230,266).

Claims 2 and 14

Since claims 2 and 14 respectively depend from claims 1 and 13, and since Appellants have argued *supra* that claims 1 and 13 are not unpatentable over Lewis in view of Weinstein, Appellants maintain that claims 2 and 14 are likewise not unpatentable over Lewis-Weinstein and further in view of Perlman.

In addition with respect to claims 2 and 14, Appellants maintain that Lewis-Weinstein and further in view of Perlman does or suggest not teach the following first feature: "wherein the SCAC certificate is obtained by the server whenever the certifying authority invalidates its public key".

The Examiner's Answer states: "Lewis does not disclose a Certificate Authority (CA) that invalidates or withdraws its public/private key. However, Penman discloses Certificate Authority (CA) that invalidates or withdraws its public/private key pair through the process of revocation."

In response, Appellants note that Perlman repeatedly discusses certificate revocation. However, Perlman does not teach or suggest public key invalidation, and the Examiner's Answer has not produced a citation that allegedly discloses public key invalidation, as required by claims

2 and 14.

The Examiner's Answer, page 20 (Point B.1) states: "The revocation of a public/private key is analogous to the invalidation of a certificate and its public/private key pair. The reason for the revocation can be an expired key pair, compromise of a key pair, or any other reason the certificate authority is required to invalidate or revoke the public/private key pair and its attached certificate."

In response, Appellants contend that the preceding argument on page of the Examiner's Answer is not persuasive, because the Examiner has not cited anything in Perlman that allegedly discloses revocation of a public/private key. Appellants assert that Perlman discloses certificate revocation and does not disclose revocation of a public/private key.

In addition with respect to claims 2 and 14, Appellants maintain that Lewis in view of Perlman does not teach or suggest the second feature: "contacting the certifying authority using the server's private key for authentication **to make a request** for the SCAC certificate" (claim 2) (emphasis added), and similar language for claim 14. The Examiner's Answer argues that Perlman, col. 6, line 63 - col. 7, line 6 discloses the preceding second feature of claims 2 and 14.

In response, Appellants maintain that Perlman, col. 6, line 63 - col. 7, line 6 does not disclose "to make a request for the SCAC certificate", as alleged by the Examiner. Indeed, Perlman, col. 6, line 63 - col. 7, line 8 recites:

> "In order to update the certificates previously issued by certificate authorities 204c so as to ensure that principals relying upon such certificates now recognize the validity of certificates (including the special delegation certificate) issued by the successor CA 204b, CA 204a **may issue**, via secure off-line techniques, to certificate authorities 204c **a**

"renunciation" certificate 600 (the data structure of which is represented in FIG. 6) signed using the private key of the CA 204a including information 602 stating that the CA 204a has renounced all of its certification authority (i.e., power to issue certificates), and has granted that authority to the CA 204b" (emphasis added).

Thus, Perlman, col. 6, line 63 - col. 7, line 6 discloses issuing a renunciation certificate and most certainly does not disclose requesting the SCAC certificate. In other words, "requesting" and "issuing" are different actions. Moreover, a renunciation certificate is not a SCAC certificate.

In addition with respect to claims 2 and 14, Appellants maintain that Lewis in view of Perlman does not teach or suggest the third feature: "verifying the request by the certifying authority using the server's public key" (claim 2), and similar language for claim 14. The Examiner's Answer argues that Perlman, col. 7, lines 15-18 discloses the preceding third feature of claims 2 and 14.

In response, Appellants maintain that Perlman, col. 7, lines 15-18 does not disclose "to make a request for the SCAC certificate", as alleged by the Examiner. Indeed, Perlman, col. 7, lines 15-18 recite: "The authorities 204c receiving such renunciation certificates from CA 204a verify that the renunciation certificates have been properly signed by the CA 204a". Appellants contend that the preceding quote of Perlman discloses verifying that the renunciation certificates have been properly signed by the CA, but does not disclose verifying the request by the certifying authority using the server's public key, as required by claims 2 and 14.

In addition with respect to claims 2 and 14, Appellants maintain that Lewis in view of

Perlman does not teach or suggest the fourth feature: "generating the SCAC certificate by the certifying authority using a new private key of the certifying authority and **forwarding the SCAC certificate to the server**" (claim 2) (emphasis added), and similar language for claim 14. The Examiner's Answer argues that Perlman, col. 7, lines 12-24 discloses the preceding fourth feature of claims 2 and 14.

In response, Appellants maintain that Perlman, col. 7, lines 12-24 does not disclose "forwarding the SCAC certificate to the server" as alleged by the Examiner's Answer and as required by claims 2 and 14.

In addition, Appellants contend that the Examiner's reason for modifying Lewis by the alleged teaching of Perlman is not persuasive. The Examiner's Answer argues: "It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the inventions of Lewis to include a Certificate Authority (CA) that invalidates its key pair through the process of revocation as taught in Perlman. One of ordinary skill in the art would have been motivated to incorporate the invention of Perlman in order to ensure the authenticity of certificates when a CA invalidates a public/private key pair. (see Perlman col. 2, lines 20-26: "... *network security, every principal must have a certificate ... desirable to later disable a certificate after it has been issued but* ***prior to its expiration****. For example, a principal's private key may be stolen, compromised or lost, etc. ... revoke the certificate, thereby disabling authentication via that certificate* ...")" (emphasis added)..

In response, Appellants maintain that the cited motivation in Perlman requires revocation of the original certificate ***prior to expiration*** of the original certificate. However, with respect to

claims 1 and 13 from which claims 2 and 14 respectively depend, the Examiner's Answer cites Lewis, col. 30, lines 39-43 which requires that a condition precedent for issuance of the new certificate (alleged by the Examiner's Answer to be the SCAC certificate) is that the original certificate expires. See Lewis, col. 30, lines 39-43 (**"When a certificate expires**, the USPS certification authority will issue a new certificate ..." (emphasis added)).

Appellants contend that ordinary logic requires that the original certificate either have expired or not have expired (but not both) when the new certificate is issued by the CA. In other words, the Examiner's Answer is arguing to modify Lewis by the alleged teaching of Perlman by issuing the new certificate when the original certificate has both expired and not expired, which is logically impossible. Therefore, the Examiner's argument for modifying Lewis by the alleged teaching of Perlman is not persuasive.

Accordingly, Appellants maintain that claims 2 and 14 are not unpatentable over Lewis-Weinstein in view of Perlman.

Claims 3 and 15

Since claims 3 and 15 respectively depend from claims 1 and 13, and since Appellants have argued *supra* that claims 1 and 13 are not unpatentable over Lewis in view of Weinstein, Appellants maintain that claims 3 and 15 are likewise not unpatentable over Lewis-Weinstein and further in view of Perlman.

In addition with respect to claims 3 and 15, Appellants maintain that Lewis-Weinstein and further in view of Perlman does not teach or suggest the following feature: "wherein

generating the SCAC certificate includes authenticating the server name, the server public key, old certifying authority public key, **and** certifying authority name" (emphasis added) (claim 3), and similar language for claim 15. The Examiner's Answer argues that Perlman, col. 7, lines 10-12 disclose the preceding feature of claims 3 and 15.

In response, Appellants maintain that Perlman, col. 7, lines 10-12 does not disclose authenticating all four items (the server name, the server public key, old certifying authority public key, and certifying authority name) listed in clams 3 and 15. In fact, Perlman, col. 7, lines 10-12 recites: "Additionally, in system 200, the new CA 204b is configured to issue certificates in the same name as the CA 204a", which is not a disclosure of authenticating all four items (the server name, the server public key, old certifying authority public key, and certifying authority name).

Accordingly, Appellants maintain that claims 3 and 15 are not unpatentable over Lewis-Weinstein in view of Perlman.

GROUND OF REJECTION 3

Claim 4 stands rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Lewis-Weinstein and further in view of Kramer *et al.* (US Patent No. 6,324,525).

Since claim 4 depend from claim 1, and since Appellants have argued *supra* that claim 1 is not unpatentable over Lewis in view of Weinstein, Appellants maintain that claim 4 is likewise not unpatentable over Lewis-Weinstein and further in view of Kramer .

In addition with respect to claim 4, Appellants maintain that Lewis-Weinstein and further in view of Kramer does not teach or suggest the feature: "issuing by the certifying authority a client (CCAC) certificate, said CCAC certificate being functionally the same as the SCAC certificate subject to the roles of the browser and the server being interchanged".

The Examiner's Answer argues: "Lewis does not specifically disclose the usage of a Certificate Authority (CA) issuing client and server type certificates. However, Kramer discloses the method of claim 1 further comprising issuing by the certifying authority a client (CCAC) certificate, said CCAC certificate being functionally the same as the SCAC certificate subject to the roles of the browser and the server being interchanged. (see Kramer col. 105, lines 61-62; col. 105, line 66- col. 106, line 1; col. 90, lines 27-31: Certificate Authority (CA) for certificate issuance; col. 17, lines 43-47; col. 17, Lines 27-30: client and server type certificates) ... It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Lewis to enable the usage of client and server certificates utilizing a trusted third party designated a certificate authority for certificate issuance as taught by Kramer. One of ordinary skill in the art would be motivated to employ Kramer in order to enable secure communications over the publicly access network such as the Internet communications network. (see Kramer col. 4, lines

19-21: "... critical that any solution utilizing the Internet for a communication backbone employ some form of cryptography ... "

In response, Appellants contend that Kramer (col. 105, lines 61-62; col. 105, line 66- col. 106, line 1; col. 90, lines 27-31; col. 17, lines 43-47; col. 17, lines 27-30) does not even come close to disclosing the preceding feature of claim 4. The Examiner's Answer has not provided any analysis to demonstrate that the Examiner's citations teach or suggest the preceding feature of claim 4.

In further response, Appellants contend that the Examiner's argument for modifying Lewis by the alleged teaching of Kramer (i.e., "in order to enable secure communications over the publicly access network such as the Internet communications network") is not persuasive because Lewis' invention already achieves secure communications over the Internet without employing the alleged teaching of Kramer.

See Lewis, col. 2, lines 6-8 ("It is, therefore, an object of the present invention to provide customer (client) to remote service provider (server) electronic transactions which are **secure** and reliable. "). See Lewis, col. 2, lines 23-28 ("The present invention ... is directed to an application which can be downloaded from the Internet, extracted from a zip file, installed, accessed by a pre-registered user on a **secure PC**, and used to conduct electronic commerce. "). See Kramer, col. 8, lines 11-12 ("The inbound network 110 allows a customer 2n to securely access the RSP web server 150."). Indeed, most of the Lewis disclosure is devoted to techniques for achieving secure communications over the Internet.

Therefore, a person of ordinary skill in the art would not be motivated to modify Lewis by the alleged teaching of Kramer "to enable secure communications over the publicly access

network such as the Internet communications network".

Accordingly, Appellants maintain that claim 4 is not unpatentable over Lewis-Weinstein in view of Kramer.

GROUND OF REJECTION 4

Claim 16 stands rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Lewis-Weinstein and further in view of Kramer *et al.* (US Patent No. 6,324,525).

Since claim 16 depend from claim 13, and since Appellants have argued *supra* that claim 13 is not unpatentable over Lewis in view of Weinstein, Appellants maintain that claim 16 is likewise not unpatentable over Lewis-Weinstein and further in view of Kramer.

In addition with respect to claim 16, Appellants maintain that Lewis-Weinstein and further in view of Kramer does not teach or suggest the following feature: "means for issuing by the certifying authority a client(CCAC) certificate, said CCAC certificate being functionally the same as the SCAC certificate subject to the roles of the browser and the server being interchanged" (emphasis added).

The Examiner's Answer argues: "Lewis does not specifically disclose the usage of a Certificate Authority issuing client and server type certificate. However, Kramer discloses the system of claim 15, further comprising means for issuing by the certifying authority a client (CCAC) certificate, said CCAC certificate being functionally the same as the SCAC certificate subject to the roles of the browser and the server being interchanged. (see Kramer col. 105, lines 61-62; col. 105, line 66 - col. 106, line 1; col. 90, lines 27-31: Certificate Authority (CA) for certificate issuance; col. 17, lines 43-47; col. 17, lines 27-30: client and server certificates) ... It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Lewis to enable the usage of client certificates and server certificates utilizing a trusted third party designated a certificate authority for certificate issuance as taught by Kramer. One of ordinary skill in the art would be motivated to employ Kramer in order to enable secure

communications over the publicly access network such as the Internet communications network. (see Kramer col. 4, lines 19-21)".

In response, Appellants contend that Kramer (col. 105, lines 61-62; col. 105, line 66- col. 106, line 1; col. 90, lines 27-31; col. 17, lines 43-47; col. 17, lines 27-30) does not even come close to disclosing the preceding feature of claim 16. The Examiner's Answer has not provided any analysis to demonstrate that the Examiner's citations teach or suggest the preceding feature of claim 16.

In further response, Appellants contend that the Examiner's argument for modifying Lewis by the alleged teaching of Kramer (i.e., "in order to enable secure communications over the publicly access network such as the Internet communications network") is not persuasive because Lewis' invention already achieves secure communications over the Internet without employing the alleged teaching of Kramer.

See Lewis, col. 2, lines 6-8 ("It is, therefore, an object of the present invention to provide customer (client) to remote service provider (server) electronic transactions which are **secure** and reliable. "). See Lewis, col. 2, lines 23-28 ("The present invention ... is directed to an application which can be downloaded from the Internet, extracted from a zip file, installed, accessed by a pre-registered user on a **secure PC**, and used to conduct electronic commerce. "). See Kramer, col. 8, lines 11-12 ("The inbound network 110 allows a customer 2n to securely access the RSP web server 150."). Indeed, most of the Lewis disclosure is devoted to techniques for achieving secure communications over the Internet.

Therefore, a person of ordinary skill in the art would not be motivated to modify Lewis by the alleged teaching of Kramer "to enable secure communications over the publicly access

network such as the Internet communications network".

Accordingly, Appellants maintain that claim 16 is not unpatentable over Lewis-Weinstein in view of Kramer.

SUMMARY

In summary, Appellant respectfully requests reversal of the August 11, 2004 Office Action rejection of claims 1-6 and 11-19. The Director is hereby authorized to charge and/or credit Deposit Account No. 09-0457.

Respectfully submitted,

Jack P. Friedman

Jack P. Friedman
Attorney For Appellant
Registration No. 44,688

Dated: 12/11/2006

Schmeiser, Olsen & Watts
3 Lear Jet Lane - Suite 201
Latham, New York 12110
(518) 220-1850